Les obligations générales du responsable du traitement et la place du sous-traitant

Delforge, Antoine

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 8
Les obligations générales du responsable du traitement et la place du sous-traitant[1]

Antoine DELFORGE[2]

« Un grand pouvoir implique de grandes responsabilités. »[3]

Introduction

1. Le RGPD ne révolutionne pas les principes fondamentaux de la protection des données à caractère personnel. Néanmoins, en œuvrant à responsabiliser davantage les responsables de traitement et les sous-traitants, le RGPD modifie substantiellement la façon d'appréhender la conformité à la réglementation relative à la protection des données. Un nouveau principe clé voit donc le jour, le principe d'« *accountability* ». L'idée derrière ce terme emprunté à la langue anglaise est de laisser plus de marge de manœuvre aux responsables de traitement et à leur(s) sous-traitant(s) pour assurer la conformité de leurs traitements avec le cadre légal applicable à ceux-ci, tout en exigeant de ces derniers d'être en mesure de pouvoir démontrer, prouver, cette conformité. De ce principe clé, découlent également d'autres nouveaux principes, eux aussi mieux connus en anglais, le principe de « *privacy by design* » et le principe de « *privacy by default* » qu'il reviendra aux différents responsables de traitement d'intégrer dans leur politique de mise en conformité.

Le responsable du traitement demeure donc l'acteur majeur de cette conformité et il se doit de s'assurer que les traitements de données qu'il effectue respectent bien le RGPD.

[1] Nous tenons à remercier Karen Rosier pour sa relecture attentive et ses précieux conseils.

[2] Chercheur au Centre de Recherche Information, Droit et Société (CRIDS), de l'Université de Namur

[3] J. SIMON *et al.*, « Spiderman », in *Amazing Fantasy # 1*, Manhattan, Marvel Comics, 1962.

2. Au travers de cette contribution, nous tâcherons de faire comprendre ces nouveaux principes qui sont en réalité à l'origine même d'une série d'autres nouvelles obligations incombant aux responsables de traitants et aux sous-traitants[4].

Afin d'appréhender ces nouveaux principes plus en détail et de mesurer l'impact de ces derniers sur la relation entre les différents acteurs d'un traitement de données, nous nous attarderons sur la notion même de responsable du traitement, de responsable conjoint, de sous-traitant et nous étudierons comment le RGPD tente de formaliser ces relations afin de répartir de manière transparente les obligations de chacun et ainsi mieux responsabiliser les acteurs.

CHAPITRE 1. La notion de « responsable du traitement » et de « sous-traitant »

SECTION 1. – Introduction

3. Les définitions de « responsable du traitement » et de « sous-traitant » n'ont pas changé entre la Directive et le règlement. L'article 4, 7) et 8), du RGPD reprennent quasiment mot pour mot les termes de l'article 2, d) et e), de la Directive.

Avec l'entrée en vigueur de la Directive, ces notions sont devenues des notions communautaires, ce qui signifie qu'elles deviennent des concepts européens autonomes et indépendants de toutes dispositions nationales[5].

4. Depuis déjà plusieurs années, les traitements de données ne se font plus en vase clos. Le développement des nouvelles technologies de communication a fait émerger de nouvelles manières de gérer ces données (en passant par du *cloud* par exemple). Dorénavant, de nombreux acteurs interviennent dans ces traitements.

De plus, les sociétés privées et les administrations ont vu leur organisation se complexifier. Il est désormais très fréquent de se retrouver face à

[4] Nous pensons notamment à l'obligation de désigner un DPO, de tenir un registre des activités de traitement… Pour une étude de ces différentes obligations, nous renvoyons aux différentes contributions traitant spécifiquement de celles-ci au sein du présent ouvrage.

[5] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, 16 février 2010, p. 9.

des groupes d'entités relativement autonomes s'échangeant régulièrement des données à caractère personnel.

Il est donc devenu plus difficile d'identifier clairement qui doit être qualifié de responsable du traitement et qui est simple sous-traitant.

5. Pour cette raison, en 2010, le Groupe 29 a rendu un avis[6] sur ces notions afin d'éviter l'apparition de divergences d'interprétation entre États membres.

Dès lors que le RGPD ne modifie pas la définition qui est faite du responsable du traitement et du sous-traitant et qu'il n'apporte pas plus de précisions sur les éléments compris dans ces définitions, l'avis du Groupe 29 reste parfaitement d'actualité.

SECTION 2. – La notion de « responsable du traitement »[7]

6. Le responsable du traitement est défini comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre »[8].

Cette définition se compose principalement de trois éléments qu'il revient d'analyser distinctement[9] :

– la personne physique ou morale, l'autorité publique, le service ou un autre organisme ;
– qui, seul ou conjointement avec d'autres[10] ;
– détermine les finalités et les moyens du traitement.

---

[6] *Ibid.*

[7] Cette section et sa structure sont librement inspirées de l'avis 1/2010 du Groupe 29 sur les notions de « responsable du traitement » et de « sous-traitant ».

[8] Art. 4, 7), du RGPD.

[9] La deuxième partie de l'article 4, 7), du RGPD règle quant à elle la question de la désignation du responsable du traitement en cas de traitement imposé par un texte juridique.

[10] Dans un souci de clarté, cet élément sera étudié en dernier.

§ 1. Premier élément : la personne physique ou morale, l'autorité publique, le service ou un autre organisme

7. Le premier élément de la définition désigne qui peut être responsable du traitement. La référence aux termes « autre organisme » montre clairement que ce premier critère doit être apprécié de manière large afin de couvrir toutes sortes d'organisations qui traiteraient des données à caractère personnel.

Tant une personne physique qu'une personne morale peuvent devenir responsables du traitement. Cependant, si une personne physique traite des données à caractère personnel dans le cadre de ses missions au sein d'une personne morale, la personne physique n'est pas considérée comme responsable de ce traitement, la personne morale demeurera seule responsable de celui-ci. Ceci s'explique par le fait que la personne physique ne met normalement pas en œuvre des opérations de traitement pour son compte propre. De plus, cela permet « aux personnes concernées de s'adresser à une entité plus stable lorsqu'elles exercent les droits qui leur sont conférés par [le Règlement] »[11].

Le fait qu'une entreprise désigne explicitement une personne comme responsable de la gestion des données n'aura pas pour conséquence de déplacer la responsabilité du traitement sur celle-ci. L'entreprise restera donc seule responsable.

8. Cependant, si une personne physique utilise les données d'une entreprise ou d'un organisme public à des fins privées, cette personne devra alors être considérée comme unique responsable pour ces nouveaux traitements[12].

Dans l'hypothèse où un employé d'une personne morale vient à utiliser des données à caractère personnel dans le cadre de ses activités professionnelles, mais sans l'autorisation de sa hiérarchie, la personne morale demeure malgré tout responsable de ce traitement.

---

[11] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, p. 16.

[12] Ceci constitue alors un détournement des finalités pour lesquelles ces données ont été récoltées, ce qui est contraire au RGPD et entraine donc la responsabilité de la personne physique. La personne morale quant à elle peut se voir reprocher un manque de mesures de sécurité, voy. art. 32, § 4, du RGPD.

§ 2. Deuxième élément : qui détermine les moyens et les finalités

a) Remarques préliminaires : « détermine »

9. Identifier qui est responsable du traitement revient à identifier qui prend les décisions importantes concernant le traitement.

Cette appréciation se fait sur la base des circonstances de fait. Pour cela, il y a lieu de voir, dans chaque cas, qui a l'autorité pour déterminer les caractéristiques principales d'un traitement : son objectif, ses méthodes...

Dès lors, les éléments contenus dans un contrat entre plusieurs parties (attribution des responsabilités de chacun) doivent être pris en compte pour apprécier sur qui repose la responsabilité du traitement, mais ces éléments doivent refléter la situation réelle. La désignation dans un contrat d'une partie comme responsable du traitement ne suffit donc pas pour qualifier celle-ci de responsable du traitement au sens du droit relatif à la protection des données. De même, se faire désigner comme sous-traitant ne permet pas non plus d'échapper aux différentes obligations attribuées au responsable du traitement. Il faudra que ces désignations correspondent aux rôles effectifs de chaque partie.

L'affaire *SWIFT*[13] en est le parfait exemple. En l'espèce, dans les contrats qui la liaient avec de nombreuses banques, la Société SWIFT était à chaque fois qualifiée de sous-traitant alors qu'elle avait un réel pouvoir de décision sur les traitements qu'elle effectuait[14] et devait dès lors être qualifiée de responsable du traitement.

Une approche formelle de la notion aurait nui gravement à l'effectivité de la législation relative à la protection des données à caractère personnel.

10. Le responsable du traitement peut également être désigné par le droit communautaire ou national. De fait, la seconde partie de l'article 4, 7), du RGPD prévoit que dans les cas où les moyens et finalités d'un traitement sont déterminés par le droit communautaire ou un droit national, il doit être précisé dans ce texte légal qui en est désigné comme responsable. Cela peut se faire directement en nommant une entité ou en indiquant les éléments pertinents pour sa désignation. Cette désignation doit évidemment être effectuée conformément aux règles d'attribution qui viennent d'être rappelées précédemment.

---

[13] À ce sujet, voy. notamment Groupe 29, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) , WP 128, 22 november 2006.

[14] Pour les cas où plusieurs entités ont un pouvoir de décision, voy. *infra*, Section 2, § 3.

De même, si un organisme se voit confier une mission légale qui nécessite *de facto* un traitement de données à caractère personnel, cet organisme sera considéré comme étant désigné par la loi responsable de ce traitement[15].

b) Détermine les finalités et les moyens

11. L'expression « détermine les finalités et les moyens » fait référence au pouvoir de décision, à l'autonomie, que doit avoir une partie pour être qualifiée de responsable du traitement.

Concrètement, déterminer les finalités d'un traitement signifie définir les objectifs de celui-ci, et déterminer les moyens se réfère à la manière d'y parvenir : le « pourquoi » et « le comment »[16].

Par « moyens », il faut entendre moyens techniques, moyens qui peuvent en principe être décidés par un sous-traitant. Cependant, derrière ce terme peuvent se cacher également d'autres éléments essentiels « réservés à l'appréciation du responsable du traitement, tels que "quelles sont les données à traiter ?", "pendant combien de temps doivent-elles être traitées ?", "qui doit y avoir accès", etc. »[17].

Ces deux éléments sont évidemment liés, il est en effet impossible de décider d'effectuer un traitement sans avoir un minimum réfléchi à la manière d'y parvenir.

12. Pour être qualifié de responsable du traitement, il n'est pas nécessaire de déterminer les finalités et les moyens dans les moindres détails. Il suffit d'avoir un certain degré d'influence sur l'un de ceux-ci.

Concernant la détermination de la finalité d'un traitement, l'arbitrage est assez simple. Toute personne qui détermine la finalité de ce traitement est *de facto* responsable du traitement puisqu'elle a un pouvoir de décision sur un élément essentiel du traitement. À l'inverse, un sous-traitant ne peut par lui-même déterminer une finalité sans sortir de son rôle de simple exécutant.

Quant à la détermination des moyens à mettre en place, l'évaluation est plus complexe puisqu'il est devenu très fréquent de faire appel à des sous-traitants à qui est souvent laissée une certaine marge de manœuvre dès lors qu'il s'agit de prestataires souvent plus spécialisés que le responsable du traitement lui-même. La question est donc de savoir à partir de quand un sous-traitant ayant reçu des consignes très vagues sur les moyens techniques et organisationnels à adopter peut devenir responsable conjoint

[15] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, p. 11.
[16] *Ibid.*, p. 14.
[17] *Ibid.*, p. 15.

de ce traitement. Dans son avis n° 1/2010, le Groupe 29 a précisé que « la détermination des moyens impliquerait une responsabilité uniquement lorsqu'elle concerne les éléments essentiels des moyens »[18].

Ainsi, le sous-traitant à qui on laisse le choix du matériel informatique utilisé n'est pas considéré comme responsable du traitement. La situation serait par exemple différente si ce dernier décidait dans quel pays les données sont stockées.

Précisons qu'un sous-traitant n'ayant reçu aucune indication sur les moyens techniques et organisationnels se devra d'utiliser des moyens raisonnables et relativement prévisibles pour le responsable du traitement et informer celui-ci de ces choix.

§ 3. Troisième élément : seul ou conjointement

13. La responsabilité d'un traitement de données peut reposer sur une ou plusieurs personnes. Dans les cas où les finalités et les moyens du traitement sont déterminés par plusieurs entités juridiques distinctes, toutes celles-ci seront responsables conjoints du traitement qu'elles mettent en œuvre. Cette idée de co-responsabilité déjà présente dans la Directive à travers ce terme « conjointement » est clairement reprise par le RGPD qui précise, si nécessaire, que « lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement »[19].

La responsabilité conjointe ne se limite pas au cas où « les entités déterminent conjointement et partagent l'ensemble des finalités et des moyens des opérations de traitement »[20].

Il existe en effet d'autres formes de responsabilité conjointe. Il arrive régulièrement que plusieurs entreprises partagent les mêmes moyens pour des finalités propres. Elles seront dans ce cas responsables conjoints des moyens utilisés pour récolter ces données mais resteront chacune seule responsable du traitement subséquent de ces données. Imaginons, par exemple, le cas de plusieurs bibliothèques qui décident de mettre en place une base de données commune afin de s'échanger l'identité de clients en situation de non restitution d'ouvrages. Les différentes bibliothèques assument la responsabilité de la gestion globale de cette base de données (sa sécurité notamment) mais chacune d'entre elles est responsable des traitements qu'elle effectue sur ces données dans le cadre de son activité.

---

18 *Ibid.*

19 Art. 26, § 1, du RGPD.

20 Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, p. 23.

Dans d'autres cas, chaque entité traite seule l'une à la suite de l'autre les mêmes données. Si à première vue on peut considérer que chaque entité détermine seule les moyens et les finalités de son traitement, il faut également « vérifier si, d'un point de vue global, les opérations de traitement ne doivent pas être considérées comme un "ensemble d'opérations" poursuivant une finalité commune ou utilisant des moyens déterminés conjointement »[21,22].

14. Cette responsabilité conjointe n'est pas sans poser de difficultés. Elle rend en effet les choses plus complexes et donc moins transparentes pour la personne concernée qui se retrouve face à plusieurs interlocuteurs qui auront parfois tendance à se renvoyer la balle en cas de demande ou si leur responsabilité est engagée.

Faire reposer la responsabilité sur plusieurs entités a d'ailleurs parfois fait craindre que « la protection des données à caractère personnel ne soit affaiblie ou qu'un "conflit négatif de compétence" et des failles n'apparaissent, auquel cas certaines obligations ou droits découlant de la directive ne seraient assumés par aucune des parties »[23].

Afin d'éviter ce jeu de ping-pong, le RGPD prévoit explicitement que la personne concernée peut exercer ses droits auprès du responsable du traitement de son choix[24], et notamment lui réclamer la réparation d'un dommage qu'elle aurait subi à la suite d'une violation du RGPD, charge à lui de se retourner ensuite contre les autres responsables conjoints s'il le souhaite[25].

De plus, le RGPD précise que les responsables conjoints doivent définir conjointement leurs obligations respectives[26].

SECTION 3. – La notion de « sous-traitant »

15. Au sens du RGPD[27], un sous-traitant est une « personne physique ou morale, [une] autorité publique, [un] service ou tout autre organisme

[21] *Ibid.*, p. 22.

[22] Pour d'autres scénarii de responsabilité conjointe, voy. Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, pp. 20 et s.

[23] *Ibid.*, p. 24.

[24] Art. 26, § 3, du RGPD.

[25] Voy. art. 82 du RGPD. Nous renvoyons à ce sujet à la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

[26] Art. 26, § 1, du RGPD. À ce sujet, voy. *infra*, Chapitre 5.

[27] Le règlement reprend exactement la même définition que la Directive.

qui traite des données à caractère personnel pour le compte du responsable du traitement »[28].

Cette définition contient deux conditions : avoir une personnalité juridique distincte de celle du responsable du traitement et traiter les données pour le compte de celui-ci[29].

16. Pour remplir la première condition (avoir une personnalité juridique distincte), il ne suffit pas que le « sous-traitant » ait une personnalité juridique propre, mais encore faut-il que ce « sous-traitant » soit une organisation extérieure à celle du responsable du traitement[30], et dispose donc d'une existence propre et indépendante, qu'il ne soit pas entièrement intégré au fonctionnement interne du responsable du traitement. Ainsi, un médecin hospitalier n'étant pas lié par un contrat de travail avec l'hôpital dans lequel il pratique n'est pas pour autant sous-traitant de cet hôpital puisque « ses activités sont totalement intégrées dans celles de l'hôpital »[31].

17. Ensuite le sous-traitant doit « agir pour le compte d'un tiers ». « Agir pour le compte d'un tiers » signifie « servir les intérêts d'un tiers et renvoie à la notion juridique de délégation »[32]. Le sous-traitant se contente d'« exécuter les instructions données par le responsable du traitement, au moins en ce qui concerne la finalité du traitement et les éléments essentiels des moyens »[33]. Si le sous-traitant dispose d'une large marge de manœuvre, à tel point qu'il prend concrètement part à la détermination des finalités poursuivies par le traitement ou décide lui-même des éléments essentiels (techniques ou organisationnels) mis en place pour y parvenir, celui-ci devra être requalifié en responsable conjoint de ce traitement, et devra donc en assumer la pleine responsabilité[34]. Cette possibilité de requalifier certains acteurs, eu égard aux circonstances concrètes dans lesquelles le traitement a été imaginé et conçu, était déjà possible

---

[28] Définition du terme « sous-traitant » donnée à l'article 4, 8), du RGPD.

[29] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, p. 27.

[30] *Ibid.*

[31] J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », in *Law, Norms and Freedoms in cyberworld / Droit, Normes et Libertés dans le cybermonde* (E. Degrave, C. de Terwangne, S. Dusollier et R. Queck coord.), coll. CRIDS, Bruxelles, Larcier, 2018, p. 748.

[32] Groupe 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », précité, p. 27.

[33] *Ibid.*

[34] *Ibid.*

avant l'adoption du RGPD[35]. La nouveauté est qu'elle est désormais explicitement prévue à l'article 28, paragraphe 10, du règlement.

18. Le sous-traitant et les personnes agissant sous son autorité (son propre sous-traitant notamment)[36] ne peuvent donc pas traiter ces données pour d'autres finalités que celles prévues par le responsable du traitement ou contrairement aux instructions reçues de ce dernier, à moins d'y être obligés légalement[37]. Le sous-traitant est d'ailleurs chargé de prendre les mesures nécessaires pour empêcher les personnes ayant accès à ces données de les réutiliser illégalement[38].

Néanmoins, si cela devait arriver, ces personnes seraient considérées comme responsables de traitement pour ce nouveau traitement qu'elles ont initié.

De même, un sous-traitant qui déciderait de ne pas respecter les instructions du responsable du traitement ou qui suivrait des instructions de celui-ci qu'il sait être illicites engagerait sa responsabilité civile et serait donc tenu personnellement de dédommager le préjudice causé par le traitement qui constitue une violation du règlement[39].

19. Rappelons que, pour être sous-traitant au sens du RGPD, il faut encore « traiter des données personnelles », c'est-à-dire être en charge d'opération(s) sur des données à caractère personnel[40]. Un vendeur de solutions logicielles ou de caméras de surveillance n'est donc pas un sous-traitant dans la mesure où il ne fait que mettre à disposition un matériel – un moyen de traitement – qui sera utilisé uniquement par l'acquéreur. La situation est différente si le logiciel fonctionne partiellement via le *cloud*[41] (pour le volet hébergement des données par exemple), auquel cas

---

[35] *Ibid.*

[36] Sur les spécificités liées au cas de la sous-traitance en cascade, voy. *infra*, Chapitre 6, Section 3, § 3.

[37] Art. 29 du RGPD.

[38] Art. 32, § 4, du RGPD.

[39] Art. 82, § 2, du RGPD. Nous vous renvoyons à ce sujet à la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

[40] Voy. art. 4, 2), du RGPD. Nous vous renvoyons à ce sujet à la contribution de C. de Terwangne, intitulée « Définitions clés et champ d'application du RGPD » au sein du présent ouvrage.

[41] Pour une étude des différentes formes de services de *cloud* et l'impact que cela peut avoir sur la qualification de « sous-traitant », voy. J.-M. Van Gyseghem, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, 2011, pp. 35-50 ; Groupe 29, Avis 5/2012 sur l'informatique en nuage, WP 196, 1er juillet 2012 ; J. Herveg et J.-M. Van Gyseghem, « Un nouveau métier de la santé : la sous-traitance des données du patient », *op. cit.*, pp. 751 et s.

la personne qui gère ce *cloud* (souvent le fournisseur de logiciel lui-même) doit probablement être considérée comme sous-traitant pour certains traitements de données opérés grâce à ce logiciel.

SECTION 4. – Conclusion préliminaire

20. Si d'un point de vue théorique les trois critères sont relativement simples à cerner, en pratique définir le ou les responsable(s) d'un traitement reste un exercice délicat dès que plusieurs acteurs interviennent dans un traitement de données. Cette difficulté s'explique aisément par le caractère avant tout factuel des critères utilisés. « Qui a *in concreto* le pouvoir de déterminer les moyens et les finalités d'un traitement ? » revient en effet – dans certaines situations complexes, avec des acteurs plus puissants que d'autres – à parfois demander non pas « qui contrôle *quoi* ? », mais « qui contrôle *qui* ? ». Tel est par exemple le cas de traitements opérés par certaines filiales se conformant aux directives de leur société mère.

Cette complexité est très bien illustrée par l'affaire récente concernant les Fan Pages Facebook dans laquelle la Cour de justice a été amenée à répondre à la question de savoir si un administrateur d'une Fan page Facebook est responsable conjoint, avec Facebook, des traitements opérés par le réseau social à l'occasion de la consultation de la Fan Page[42].

CHAPITRE 2. L'obligation pour le responsable du traitement d'être « accountable »

SECTION 1. – L'introduction du principe d'« *accountability* » en matière de protection des données

21. Le RGPD a introduit un nouveau principe en matière de protection des données, le principe d'« *accountability* »[43].

[42] C.J.U.E., arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 juin 2018, C-210/16, et concl. Av. gén. Y. Bot.

[43] Art. 5, § 2, du RGPD en tant que principe général du règlement, et art. 24 du RGPD en tant qu'obligation pour le responsable du traitement.

À partir du 25 mai 2018, le responsable du traitement doit être « *accountable* » ou pour le dire en français, le responsable du traitement doit être « en mesure de rendre des comptes »[44].

Si comme nous venons de le dire, le concept d'« *accountability* » n'était pas présent dans la Directive, ou du moins pas explicitement, ce concept n'est pas pour autant neuf et apparait déjà en 1980 dans les lignes directrices de l'OCDE régissant la protection de la vie privée[45].

Il faudra toutefois attendre 2009-2010, à l'occasion de travaux du Groupe 29 sur la révision de la Directive[46], pour que ce concept devienne celui que l'on connait actuellement dans le RGPD.

Ce nouveau principe d'« *accountability* » vise à davantage responsabiliser les responsables de traitement en leur laissant plus de marge de manœuvre dans les choix qu'ils posent afin d'assurer la conformité de leur traitement avec le RGPD.

22. Dans cette optique, un changement de paradigme s'effectue, en passant d'un modèle de contrôle *a priori* (lourd et peu efficace[47]) à un modèle de contrôle *a posteriori*.

Ce basculement entraine trois conséquences :

– suppression d'un certain nombre de formalités préalables au traitement ;
– responsabilisation des responsables de traitement ;
– renforcement des pouvoirs de contrôle et de sanction[48].

Le responsable du traitement a donc plus de liberté qu'auparavant concernant les mesures à mettre en place pour assurer le respect du cadre légal, mais il est responsable de ses choix et doit pouvoir démontrer qu'il a bien fait le nécessaire[49]. Cette plus grande flexibilité permet également

[44] Par souci de facilité et du fait que le concept d'« *accountability* » est un concept anglo-saxon relativement connu et difficilement traduisible, nous continuerons dans notre contribution à utiliser ce terme anglais.

[45] « Tout maitre de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessous », voy. OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 23 septembre 1980, art. 14.

[46] Groupe 29, Avis 3/2010 sur le principe de la responsabilité, WP 173, 13 juillet 2010 ; Groupe 29, The future of Privacy : Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data, WP 168, 1er décembre 2009.

[47] Voy. considérant n° 89 du RGPD.

[48] Nous renvoyons à ce sujet à la contribution de L. Gerard, intitulée « Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? » au sein du présent ouvrage.

[49] Pour une étude plus détaillée de l'approche du Groupe 29 sur la question, voy. Groupe 29, Avis 3/2010 sur le principe de la responsabilité, précité, pp. 1 à 9 spécifiquement.

à chaque responsable du traitement de développer les procédures les plus adaptées aux spécificités du traitement qu'il effectue.

23. Le responsable du traitement est certes plus responsabilisé, mais le RGPD ne le laisse pas complètement libre sur la manière de se conformer au règlement et impose certaines mesures qui sont particulièrement importantes et nécessaires. Nous pensons notamment à l'obligation pour le responsable de tenir un registre, d'effectuer des analyses d'impact, de désigner un DPO, de respecter les principes de « *privacy by design* » et « *privacy by default* », de recourir à des BCR (*Binding Corporate Rules*)[50]…

Le principe d'« *accountability* » n'est, pour ainsi dire, jamais cité dans le RGPD. Il n'empêche que bon nombre de mécanismes présents dans le RGPD découlent d'une manière ou d'une autre de ce principe.

SECTION 2. – L'« accountability » en tant qu'obligation générale pour le responsable du traitement

24. Si le principe d'« *accountability* » est déjà repris à l'article 5, paragraphe 2, du RGPD en tant que nouveau principe clé en matière de protection des données, il faut se tourner vers l'article 24 pour mieux comprendre ce concept un peu vague une fois qu'il faut le mettre en pratique.

L'article 24 énonce les deux éléments de base du principe d'« *accountability* » puisqu'il prévoit que « […] le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées **pour s'assurer** et **être en mesure de démontrer** que le traitement est effectué conformément au présent règlement »[51].

§ 1. Mettre en œuvre des mesures adéquates pour respecter le RGPD

25. Le responsable du traitement doit donc mettre en place des mesures techniques et organisationnelles appropriées et efficaces[52] pour s'assurer que les traitements qu'il effectue respectent le RGPD. Pour apprécier cette efficacité et apporter les solutions techniques et organisationnelles

[50] Nous renvoyons pour ces différentes obligations aux autres contributions dans cet ouvrage qui traitent spécifiquement de ces sujets.

[51] Mis en gras par nos soins.

[52] Terme employé dans le considérant n° 74 du RGPD pour parler de ces mesures.

adéquates, le responsable du traitement devra notamment prendre en compte le type et le contexte du traitement, la nature des données (données sensibles ou non), les finalités poursuivies et les risques que font peser ce traitement sur les droits et libertés des personnes physiques[53]. Ainsi, sur la base de ces éléments, il sera à même de développer des mesures protectrices adaptées à la situation.

26. Cette évaluation des risques et des mesures censées les empêcher ou les diminuer à un niveau acceptable se confondra parfois avec l'analyse d'impact prévue à l'article 35 du RGPD[54]. Si cette disposition n'impose pas cette analyse pour tous les traitements, une analyse minimale est dans tous les cas nécessaire pour apprécier l'adéquation des mesures mises en place avec les risques encourus pour les personnes concernées.

27. Afin d'apprécier cette adéquation, ces mesures devront être régulièrement réévaluées et mises à jour[55].

Conformément à l'article 24, paragraphe 2, du RGPD, « lorsque cela est proportionné au regard des activités de traitement », le responsable du traitement mettra en œuvre « des politiques appropriées en matière de protection des données ». Sur ce que recouvre cette expression, nous rejoignons la position des représentants espagnols lors des travaux préparatoires qui trouvaient que « le concept d'"*appropriate data protection policies*" était trop vague »[56].

28. Une série d'autres mesures envisageables sont directement contenues dans le RGPD. Certaines sont obligatoires pour tout traitement (la mise en place de procédés visant à appliquer les principes de « *privacy by design* » et « *privacy by default* »), d'autres non. Ainsi, effectuer une analyse d'impact ou nommer un DPO n'est pas systématiquement obligatoire. Même lorsqu'elles ne sont pas exigées, ces mesures peuvent être adoptées à titre de bonnes pratiques.

---

[53] Le considérant n° 75 du RGPD liste une série de risques pour les droits et libertés des personnes physiques.

[54] Nous renvoyons à ce sujet à la contribution de F. Dumortier, « La sécurité des traitements de données à caractère personnel, les analyses d'impacts et la violation des données » au sein du présent ouvrage.

[55] Art. 24, § 1, *in fine* du RGPD.

[56] Traduction libre, voy. art. 26, note 193 du Proposal from the Council for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), doc. 17831/13, 16 décembre 2013, p. 113.

Le Groupe 29 donne quelques illustrations dans son avis de 2010 sur la notion d'« *accountability* »[57]. Nous citerons, à titre d'exemples de mesures organisationnelles, la formation de son personnel aux grands principes de la protection des données, la mise en place de procédures de gestion des demandes découlant des droits conférés aux personnes concernées, les procédures de notification en cas de violation de données et la mise en place d'audits internes ou externes permettant de tester le fonctionnement de ces différentes procédures.

Pour les mesures relatives à la sécurité des données, l'article 32 énumère quelques techniques comme le chiffrement et la pseudonymisation des données[58].

§ 2. Pouvoir démontrer la conformité des traitements

29. Le responsable du traitement doit non seulement mettre en place les mesures nécessaires afin d'assurer le respect du règlement, mais il doit également pouvoir le démontrer.

Concrètement, cela signifie que le responsable du traitement a l'obligation de documenter les traitements qu'il effectue, d'expliquer les choix qu'il pose et de garder les preuves des mesures techniques et organisationnelles qu'il a prises.

En cas de contrôle par une autorité de protection des données, le responsable du traitement sera amené à démontrer qu'il réalise des traitements de données de manière conforme au règlement. Il devra donc, par exemple, justifier (documents à l'appui) pourquoi il a considéré qu'il ne devait pas désigner de DPO. Pour ce faire, il pourrait notamment donner à l'autorité de protection des données une note détaillée, dans laquelle il précise les raisons de son choix de ne pas désigner de DPO.

30. Cette obligation de pouvoir démontrer sa conformité au RGPD facilite fortement le travail des autorités de protection de données qui n'ont plus qu'à demander au responsable du traitement les preuves de sa « compliance ».

L'important pour le responsable du traitement est donc bien de montrer qu'il s'est posé les bonnes questions, qu'il y a répondu de manière consciencieuse et qu'il a dès lors pris les mesures nécessaires pour se conformer au RGPD.

---

[57] Groupe 29, Avis 3/2010 sur le principe de la responsabilité, précité.

[58] Pour ces aspects liés à la sécurité nous renvoyons à nouveau à la contribution de F. DUMORTIER au sein du présent ouvrage.

31. Dans l'idée de pouvoir prouver le respect de ce cadre réglementaire, appliquer un code de conduite certifié ou recourir à des mécanismes de certification « peut servir d'élément attestant du respect des obligations incombant au responsable du traitement »[59].

Notons que dans sa version finale[60], le RGPD ne prévoit pas de sanction administrative pour la violation de l'article 24. Cependant l'article 24 n'est qu'une explication plus détaillée du principe d'« *accountability* » déjà présent à l'article 5 dont la violation peut quant à elle entrainer les sanctions les plus lourdes[61]. Dès lors, il y a fort à parier qu'un responsable du traitement qui ne pourrait apporter à suffisance les preuves de sa conformité au RGPD ne s'expose pas à des sanctions administratives sur la base de la violation de l'article 24, mais bien sur la base de la violation d'un principe clé du RGPD contenu à l'article 5.

32. La question qui demeure reste de savoir si ce nouveau principe d'« *accountability* » signifie qu'en cas de possible manquement du responsable du traitement, la personne concernée qui souhaiterait réclamer le dédommagement du préjudice qu'elle a subi à cause de ce manquement n'assumerait plus la charge de la preuve de ce manquement et qu'il reviendrait au responsable du traitement de prouver qu'il n'a pas violé les dispositions du RGPD. À nos yeux, le principe d'« *accountability* » ne doit pas aller jusqu'à renverser la charge de la preuve. Il faciliterait simplement l'administration de celle-ci puisque le responsable du traitement aura en principe documenté ses choix et ses procédures de sorte que le juge amené à statuer aura donc normalement toutes les pièces nécessaires à sa disposition[62].

CHAPITRE 3. Le principe de « *privacy by design* »

33. Trop souvent, la question de la mise en place des mesures nécessaires afin d'assurer le respect de la réglementation relative à la protection des données était vue comme une étape supplémentaire venant s'ajouter au processus de développement d'un service, d'un produit qui requérait des

[59] Art. 24, § 3, du RGPD.

[60] Contrairement à ce qui était prévu dans la proposition du 25 janvier 2012.

[61] Art. 83, § 5, a), du RGPD.

[62] Pour les questions de responsabilité civile du responsable du traitement, nous renvoyons à la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

traitements de données à caractère personnel. Les grands principes contenus à l'article 5 du RGPD étaient pris en compte, d'un point de vue théorique, lors de la conception du service/du produit mais, régulièrement, la mise en place de mesures techniques et organisationnelles implémentant ces principes somme toute assez théoriques ne venait qu'en second lieu, une fois le service/le produit conçu. On concevait, par exemple, un logiciel sans intégrer immédiatement et concomitamment les exigences liées à la protection des données. Ce n'était qu'ensuite que l'on réfléchissait comment le sécuriser, comment s'assurer que les personnes concernées puissent facilement avoir accès à leurs données (droit d'accès), comment elles pourraient les rectifier si nécessaire (droit à rectification).

En fonctionnant de cette manière, il arrive que, pour des raisons techniques liées à la conception de l'architecture de son logiciel ou au choix d'un logiciel plutôt qu'un autre, le responsable du traitement ne puisse, malgré sa bonne volonté, faire droit à certaines demandes légitimes de personnes concernées et donc se conformer aux exigences du RGPD. Tel était notamment le cas des demandes d'effacement. Certains responsables de traitement n'avaient en effet parfois pas les capacités techniques de localiser l'ensemble des données du demandeur et éprouvaient des difficultés à les effacer relativement rapidement.

34. Afin de remédier à cela et d'assurer la plus grande effectivité aux principes généraux en matière de protection des données, l'article 25 du RGPD impose désormais[63] à tout responsable du traitement de prendre en compte le droit de la protection des données au moment de la conception des traitements de données[64], et non à la fin de ce processus, et ainsi de mettre en place, à temps, des mesures techniques et organisationnelles appropriées pour garantir le respect des exigences du RGPD. Aux termes du considérant n° 78 du RGPD, « [ces] mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au respon-

[63] La Directive (not. à son article 17, considérant n° 46) intégrait déjà d'une certaine manière ce principe, mais le principe en tant que tel n'était pas mentionné : Groupe 29, The future of Privacy : Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data, précité, p. 13, pt 44.

[64] « Au moment de la détermination des moyens du traitement » pour reprendre l'expression contenue à l'article 25 du RGPD. Cet article continue en précisant que le responsable du traitement doit également prendre des mesures au moment du traitement lui-même.

sable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer [...] »[65].

Pour parvenir à appliquer ce principe, le responsable du traitement devrait former un minimum son personnel pour que les personnes qui, d'une manière ou d'une autre, conçoivent un nouveau traitement soient à même de penser aux aspects légaux de ce qu'ils sont en train de faire. Par ailleurs, une bonne pratique pourrait être d'organiser des processus de coopération entre les départements « métier » et le département juridique.

35. L'article 25 ne consiste donc pas uniquement à demander aux responsables de traitement d'avoir en tête ce nouveau principe de « *privacy by design* », mais bien également de les forcer à utiliser certaines techniques permettant de respecter ce principe, ce qu'on appelle les PETs (*Privacy-Enhancing-Technologies*)[66].

À titre d'exemple de PETs, citons certains logiciels permettant de flouter automatiquement les visages des personnes qui seraient filmées dans un lieu public (par une voiture intelligente[67] notamment) alors que ces personnes ne l'ont pas accepté et que connaitre l'identité de celles-ci n'est souvent pas nécessaire (intégration du principe de minimisation dans la conception même du fonctionnement du logiciel).

Concevoir des logiciels « *user-friendly* » est une forme de bonne pratique tirée du principe de « *privacy by design* » puisqu'aider l'utilisateur à mieux maitriser l'application traitant ses données va permettre au responsable de ces traitements d'être plus transparent, et à la personne concernée de pouvoir plus facilement s'informer sur les traitements opérés et faire usage des droits qui lui sont conférés par le RGPD.

---

[65] Sur le sujet, voy. les travaux de A. Cavoukian, « Information and Privacy Commissioner », Ontario, Canada, qui est à l'origine de ce concept, et particulièrement « Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices », décembre 2012, http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf ; B. Preneel et D. Ikonomou (dir.), *Privacy Technologies and Policy : First Annual Privacy Forum*, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers, Berlin, Springer, 2014.

[66] Pour plus d'informations sur différentes catégories de PETs applicables à des traitements de type « *Big data* », voy. le rapport de l'ENISA, *Privacy by design in big data : An overview of privacy enhancing technologies in the era of big data analytics*, décembre 2015, www.enisa.europa.be.

[67] Voitures utilisant une série de caméras couplées à différents logiciels afin de pouvoir circuler de manière plus ou moins autonome. Pour une application plus détaillée du principe de « *privacy by design* » au monde des robots, nous renvoyons à la contribution de A. Delforge et L. Gerard, « Notre vie privée est-elle réellement mise en danger par les robots ? : étude des risques et analyse des solutions apportées par le GDPR », in *Intelligence artificielle et droit* (A. de Streel et H. Jacquemin coord.), coll. CRIDS, Bruxelles, Larcier, 2017, pp. 143-188.

36. Pour évaluer quelles mesures sont les plus adaptées, encore une fois, le responsable du traitement devra tenir compte « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques »[68].

37. Si nous nous réjouissons de la consécration de ce principe de « *privacy by design* » qui nous parait fondamental, il n'empêche que cela n'est pas sans poser deux problèmes majeurs : que faire si le logiciel n'est pas conçu par le responsable du traitement ou si le logiciel a été conçu avant le 25 mai 2018 et dès lors n'est pas forcément « *privacy by design* » ?

Le principe de « *privacy by design* » est capital pour assurer une efficacité maximale des règles contenues dans le RGPD. Les véritables choix sont en effet posés bien souvent par les concepteurs de logiciels ou d'applications... et pas forcément par ceux qui les utilisent pour traiter des données à caractère personnel de tiers.

Dans bien des cas, les logiciels utilisés par les responsables de traitement ne sont pas développés par ceux-ci. Ils sont obtenus auprès d'une société tierce et le responsable du traitement n'en a pas supervisé la conception. Il ne maîtrise pas forcément comment le logiciel fonctionne d'un point de vue technique et n'a un aperçu que sur le volet opérationnel de ce logiciel, sur ce qu'il permet de faire, sans véritablement comprendre comment il le fait.

La manière dont les données sont traitées a été fixée en majeure partie par le concepteur et non par le responsable du traitement ignorant bien souvent les détails techniques du logiciel ou de l'application qu'il utilise.

Le véritable pouvoir est donc bien dans les mains des concepteurs. Néanmoins, juridiquement, le respect du principe de « *privacy by design* » repose sur le responsable du traitement et non sur les concepteurs qui, eux, ne traitent pas de données à caractère personnel. Ainsi, le fabricant d'un logiciel de CRM[69], par exemple, n'est pas tenu de respecter l'article 25 du RGPD imposant le principe de « *privacy by design* », seul l'utilisateur de ce logiciel – en tant que responsable du traitement – le sera. De ce fait, le concepteur de ce CRM n'a notamment pas d'obligation légale de concevoir un logiciel sécurisé[70].

---

[68] Art. 25 du RGPD.

[69] « *Customer Relationship Management* » pour « gestion de la relation client ».

[70] Sauf dans l'hypothèse où l'entreprise ayant conçu le logiciel agit non pas comme un fournisseur de logiciels qui ne traite pas lui-même de données à caractère personnel, mais comme sous-traitant (si ce logiciel fait appel par exemple à des services de *cloud* gérés par

Dès lors, bien souvent, le responsable du traitement ne pourra pas implémenter le RGPD dès la conception du logiciel, mais devra prouver qu'il a choisi un logiciel lui permettant de respecter le RGPD, c'est-à-dire un logiciel « *privacy by design* » ou « *GDPR-compliant* » pour rester dans la terminologie anglophone.

Le second problème de ce principe provient du fait que les logiciels qui sont utilisés actuellement n'ont pas toujours été pensés pour être « *privacy by design* ». Ces logiciels doivent-ils être adaptés et mis à jour[71] pour que les principes du RGPD soient mieux intégrés au sein même du fonctionnement de ces logiciels ? Selon nous, cela ne parait pas obligatoire si, au final, le traitement tel qu'il est effectué par ces logiciels est conforme aux nouveaux prescrits du RGPD. Si le logiciel n'est pas lui-même « *privacy by design* », mais que le responsable du traitement a mis en place une série d'autres mesures permettant de garantir le respect du RGPD, il n'est pas nécessaire de modifier ce logiciel.

À l'inverse, si tel n'est pas le cas, et qu'il reste des impossibilités techniques de faire droit à certaines demandes légitimes de personnes concernées par exemple, il faudra probablement faire évoluer ce logiciel et éventuellement en changer s'il est trop compliqué d'adapter celui actuellement en place.

CHAPITRE 4. Le principe de « *privacy by default* »

38. L'article 25, second paragraphe, prévoit que le responsable du traitement doit s'assurer que techniquement, *par défaut*, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement soient traitées. L'article précise par ailleurs que le responsable du traitement ne pourra dès lors pas traiter, par défaut, plus de données que nécessaire (quantité de données), plus longtemps que nécessaire (durée de conservation), et ne pourra pas non plus les rendre, par défaut, accessibles à plus de personnes que ce qui est nécessaire au vu de la finalité du traitement.

Désormais, le responsable du traitement doit donc prévoir que les données d'une personne ne seront pas rendues publiques (accessibles à un

---

cette même entreprise). Dans ce cas, en tant que sous-traitant, l'entreprise fournissant le logiciel a des obligations propres en matière de sécurité (voy. *infra*). Pour ces aspects liés à la sécurité, nous renvoyons à nouveau à la contribution de F. DUMORTIER au sein du présent ouvrage.

[71] Ann Cavoukian parle à ce sujet de « *Privacy by ReDesign* », voy. « Privacy by ReDesign : A practical framework for implementation », novembre 2011, www. Privacybydesign.ca.

nombre indéterminé de personnes physiques) si cette personne n'a pas fait, au préalable, une démarche active pour autoriser cela[72].

39. Cela signifie, concrètement, pour prendre l'exemple de certains réseaux sociaux très connus prévoyant que chaque profil d'utilisateur peut, soit être « privé » (non accessible à tiers), soit « semi-privé » (accessible à certaines personnes autorisées par la personne) soit « public » (accessible à tous les membres de ce réseau), que le profil doit *par défaut* être configuré en mode « privé » et c'est à la personne concernée, s'il elle souhaite divulguer plus ou moins largement certaines informations, de configurer à sa convenance les paramètres de son profil. Actuellement, sur un certain nombre de ces réseaux sociaux, c'est la configuration inverse qui est mise en place, à savoir que le profil est par défaut « public » et que c'est à la personne concernée de chercher dans les paramètres de son compte comment limiter la diffusion de ses informations. Ceci pose un véritable problème de transparence dans la mesure où peu de personnes sont conscientes de la publicité qui est faite de leurs données et encore plus rares sont les personnes qui font la démarche de modifier les paramètres par défaut[73].

40. Ce principe de « *privacy by default* » permet donc d'assurer, par des mesures techniques intégrées dans le fonctionnement même du logiciel, une effectivité maximale au principe de minimisation et améliore la transparence de certains traitements dont la personne concernée n'est parfois pas au courant[74]. Ce faisant, le principe de « *privacy by default* » n'est qu'une forme particulière du principe de « *privacy by design* »[75]. Si la première partie du second paragraphe de l'article 25 peut sembler n'être qu'une répétition du principe de « *privacy by design* » qu'au principe de « minimisation des données », la référence à l'accessibilité des données a le mérite de clarifier la question de savoir si le principe de « *privacy by design* » impose, en tant que tel, que les données à caractère personnel soient, par défaut, non publiques et accessibles uniquement aux personnes nécessaires au vu de la finalité du traitement.

---

[72] Art. 25, § 2, *in fine* du RGPD.

[73] Cela s'explique notamment par la difficulté qui existe souvent à accéder à ces paramètres et à comprendre comment les régler à sa convenance.

[74] En effet, parfois la personne consent à certains traitements de ses données sans véritablement saisir la portée de ceux-ci. Dès lors, imposer une véritable démarche active de la personne permet de la conscientiser un minimum.

[75] À tel point que dans ses travaux sur les 7 grands principes de la « *privacy by design* », Ann Cavoukian cite en second lieu le principe de « *privacy as the default setting* », voy. « Privacy by design : The 7 foundational principles », janvier 2011, dispo. sur www.privacybydesign.ca.

CHAPITRE 5. Les formalités obligatoires en cas de responsabilité conjointe

41. Afin d'éviter la situation où la multiplication du nombre de responsables d'un traitement peut provoquer une dilution des responsabilités, le RGPD a consacré son article 26 à ces questions de répartition des obligations entre responsables conjoints.

Cette disposition prévoit qu'en cas de responsabilité conjointe, les responsables conjoints doivent, d'un commun accord, « définir de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du règlement »[76]. À lire le second paragraphe dudit article, *de manière transparente* signifie que « les grandes lignes de l'accord [doivent être] mises à disposition de la personne concernée ». Cette formulation semble indiquer que les responsables conjoints n'ont pas l'obligation de communiquer activement à la personne concernée ces informations, mais simplement de les rendre disponibles, sur leur site internet respectif par exemple.

42. L'article 26 se poursuit en précisant que cette répartition des tâches comprend également la façon dont les différents responsables s'organiseront afin de permettre aux personnes concernées d'exercer leurs droits. Une personne de contact commune peut à cet égard être désignée conjointement pour coordonner les demandes des personnes concernées.

43. Dans cet accord, doit également être mentionné quel responsable du traitement est chargé de communiquer à la personne concernée les différentes informations visées aux articles 13 et 14 du RGPD.

44. Nous regrettons le manque de précision sur les autres éléments que doit contenir au minimum cet accord. Contrairement à ce qui est prévu pour les contrats entre responsable du traitement et sous-traitant[77], il n'est pas ici fait mention d'éléments précis à intégrer dans cet accord.

45. Les responsables conjoints peuvent en principe librement convenir ensemble de leurs obligations respectives. Néanmoins, le RGPD laisse la possibilité de définir légalement (au niveau national ou européen) les

[76] Voy. égal. considérant n° 79 du RGPD.
[77] Voy. *infra*, Chapitre 6, Section 3, § 2.

obligations respectives de chaque responsable du traitement[78]. Régler la situation de cette manière permettrait d'éviter que, dans certains cas, un des futurs responsables conjoints du traitement puisse, grâce à sa position de force, se décharger d'un certain nombre d'obligations sur son co-contractant qui est alors contraint de les assumer.

46. De plus, le contenu de l'accord doit refléter la réalité de la situation et le rôle respectif de chacun[79]. Ainsi, si un des responsables du traitement est seul gestionnaire de l'infrastructure informatique qui héberge les données, il serait logique que les obligations de notification en cas de violation de données prévues aux articles 33 et 34 du RGPD lui soient confiées. Pour prendre un autre exemple, il semblerait normal qu'un responsable conjoint qui n'a pas de contact direct avec les personnes concernées dont il traite les données n'assume pas d'obligations d'information (art. 13 et 14 du RGPD) à leur égard.

Cela signifie que cet accord sert avant tout à formaliser la relation entre les différents responsables conjoints et répartir en bonne intelligence les nombreuses obligations prévues dans le règlement.

47. Si cet accord tend à régler la relation entre responsables conjoints, il n'est nullement opposable à la personne concernée qui reste parfaitement libre de faire valoir ses droits auprès du responsable du traitement de son choix[80], charge à eux de se coordonner et mettre en place les procédures nécessaires à un traitement efficace des demandes de ces personnes.

Pour prendre l'exemple d'une demande d'accès ou d'effacement, le responsable du traitement qui aura été contacté par la personne concernée souhaitant exercer l'un de ses droits ne pourra renvoyer cette personne auprès de son co-contractant. Il devra lui-même pouvoir répondre à cette demande. Pour ce faire, il sera nécessaire qu'entre responsables conjoints, ils aient mis en place une série de procédures de coopération afin que le responsable conjoint qui aura été contacté par une personne concernée puisse relayer efficacement cette demande au responsable conjoint qui aura les capacités d'y répondre.

Cela parait normal que les responsables conjoints ne puissent limiter les choix de la personne concernée vu que celle-ci n'est pas partie à leur accord (leur contrat) et dès lors les effets internes de celui-ci lui sont non opposables. Toutefois, durant les négociations du texte, il a été proposé de limiter ce choix si « la personne concernée a été informée de

[78] Art. 26, § 1, *in fine* du RGPD.
[79] Art. 26, § 2, du RGPD.
[80] Art. 26, § 3, du RGPD.

manière transparente du responsable conjoint responsable [pour ce type de demande] »[81].

48. Nous tenons à souligner que dans le cas où un des deux responsables conjoints bénéficierait de l'exception à des fins strictement personnelles ou domestiques[82] et ne serait donc pas soumis au RGPD, l'autre responsable conjoint demeurera le seul responsable du respect du RGPD. Dès lors, dans ce cas-là, il ne nous semble pas requis de conclure un pareil accord, celui-ci n'ayant aucun sens. Le RGPD n'a malheureusement pas explicitement réglé cette situation.

CHAPITRE 6. Le rôle du sous-traitant dans le RGPD

SECTION 1. – Vers un sous-traitant plus responsable ?

49. Dans le monde informatisé qui est le nôtre, bien souvent les responsables de traitement font appel aux services de sociétés tierces pour leur permettre d'effectuer les traitements de données qu'ils souhaitent.

Comme le dit l'adage, « la résistance d'une chaîne se mesure à son maillon le plus faible ». Il est dès lors logique que le recours à un sous-traitant soit également réglementé par le RGPD, et ce de manière beaucoup plus détaillée que sous l'empire de la Directive. Si la Directive ne parlait du sous-traitant que dans une section relative à « la confidentialité et la sécurité des données »[83] et faisait reposer la quasi-totalité des obligations sur le responsable du traitement, dorénavant, le sous-traitant assume personnellement une plus grande part de responsabilité dans les traitements auxquels il participe et doit dans certains cas lui aussi, comme le responsable du traitement, tenir un registre, nommer un DPO…

[81] Traduction libre de « the data subject has been informed in a transparent manner which of the joint controllers is responsible », voy. art. 26 du Proposal from the Council the for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), doc. 17831/13, 16 décembre 2013.

[82] Art. 2, § 2, c), du RGPD. À ce sujet, nous vous renvoyons à la contribution de Cécile DE TERWANGNE, intitulée « Définitions clés et champ d'application du RGPD » au sein du présent ouvrage.

[83] Pour dire que ce dernier ne pouvait traiter les données à caractère personnel qui lui ont été confiées que sur instruction du responsable du traitement (art. 16), et qu'il était également personnellement responsable de la sécurité des traitements (art. 17).

Le sous-traitant n'est plus vu comme un simple exécutant technique, mais comme un véritable partenaire du responsable du traitement[84], qui doit être associé à différents stades du traitement. Cette plus grande responsabilisation des sous-traitants s'explique en partie par le fait que les sous-traitants sont des entreprises parfois plus importantes que les responsables de traitement pour qui elles travaillent et sont parfois les seules à avoir l'expertise suffisante pour assurer une pleine effectivité à ce nouveau règlement.

50. Cette responsabilisation accrue est particulièrement évidente lorsqu'on envisage le cas du sous-traitant d'un responsable du traitement bénéficiant de l'exception pour des activités strictement personnelles ou domestiques[85], puisque ce sous-traitant se voit tout de même imposer de respecter le RGPD[86]. À lire le considérant n° 18, un sous-traitant est en effet tenu de respecter les obligations incombant spécifiquement au sous-traitant malgré le fait que son responsable du traitement ne soit pas, lui, obligé de se conformer au RGPD. La volonté du législateur européen aura sans doute été de tenter d'imposer à ce type de sous-traitant une série d'obligations afin que les traitements de données à des fins personnelles ou domestiques effectués au moyen de leurs services soient notamment sécurisés.

51. Dans certains cas, il sera très difficile pour le sous-traitant, tel un fournisseur de service de *cloud* à destination des particuliers par exemple, de se conformer au RGPD sans (pouvoir) savoir si des données à caractère personnel (et de quelles natures) seront stockées sur ses serveurs[87]. Il convient de souligner à cet égard que ce type de sous-traitant peut également avoir la qualité d'« hébergeur » au sens de l'article 14 de la directive 2000/31/CE[88] et donc éventuellement bénéficier du régime d'exonération associé à ce statut. L'articulation entre ces deux textes est cependant particulièrement problématique[89] puisque la directive 2000/31/CE ne s'applique pas « aux

---

[84] Le sous-traitant bénéficie d'ailleurs de critères d'application propres par rapport au champ d'application territorial du RGPD. Voy. art. 3 du RGPD. À ce sujet, nous renvoyons à la contribution de C. DE TERWANGNE, intitulée « Définitions clés et champ d'application du RGPD » au sein du présent ouvrage.

[85] Art. 2, § 2, c), du RGPD.

[86] Voy. considérant n° 18 *in fine* du RGPD.

[87] M. S. VIDOVIC, « EU data protection reform : challenges for cloud computing », http://www.cyelp.com/index.php/cyelp/article/view/252, p. 181 ; K. HON, « GDPR : Killing Cloud Quickly ? », https://iapp.org/news/a/gdpr-killing-cloud-quickly/.

[88] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *J.O.U.E.*, L 178 du 17 juillet 2000.

[89] À la lecture de la Proposition de règlement de 2012, certains auteurs ont d'ailleurs souligné l'importance de mieux concilier ces deux textes, voy. not. W. K. HON, E. KOSTA, Chr. MILLARD

questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE [...] »[90] et le RGPD s'applique « sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires »[91]. L'article 2, paragraphe 4, du RGPD signifie probablement que le sous-traitant n'a pas à contrôler les données stockées sur son serveur[92]. Cette façon de tenter de concilier ces deux textes semble néanmoins en contradiction avec certaines règles prévues à l'article 28 du RGPD[93].

SECTION 2. – Le choix du sous-traitant

52. Le responsable du traitement qui envisage de faire appel à un sous-traitant ne peut choisir le sous-traitant qu'il souhaite sans prendre certaines précautions au préalable. Il a le devoir de vérifier que celui-ci « présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée »[94]. La formule ne change pas énormément de celle contenue dans la Directive, si ce n'est que l'article 17 de la Directive n'imposait qu'un contrôle des capacités techniques et organisationnelles du sous-traitant à garantir un niveau de sécurité adéquat[95]. Le règlement prévoit maintenant que le responsable du traitement doit s'assurer préalablement que le sous-traitant auquel il envisage de faire appel pourra se conformer aux exigences du RGPD et l'aider à garantir « la protection des droits de la personne concernée »[96].

---

et D. Stefanatou, « Cloud Accountability : The Likely Impact of the Proposed EU Data Protection Regulation », https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971, p. 19.

[90] Art. 1, § 5, b), de la directive 2000/31/CE.

[91] Art. 2, § 4, du RGPD.

[92] B. van Alsenoy, « Liability under EU Data Protection Law : From Directive 95/46 to the General data protection Regulation », 2017, www.jipitec.eu, sect. 3.1.4 ; nous renvoyons à ce sujet à la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

[93] Voy. *infra*, Section 3, § 2.

[94] Art. 28, § 1, du RGPD ; voy. égal. considérant n° 81 du RGPD.

[95] Art. 17 de la Directive : « Les États membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures ».

[96] Voy. art. 28, § 1, du RGPD.

Le considérant n° 81 du RGPD indique que, par « garanties suffisantes », on vise entre autres un contrôle préalable des « connaissances spécialisées », de la « fiabilité » et des « ressources » du sous-traitant. Le sous-traitant sera également amené à apporter les « garanties suffisantes » démontrant qu'il respectera ses propres obligations en tant que sous-traitant, telles que ses différentes obligations relatives à la sécurité du traitement, et dans certains cas, la nomination d'un DPO, la tenue d'un registre des activités de traitement[97]...

53. Il va de soi que le niveau d'exigences variera en fonction du type de traitement envisagé, de sorte qu'au moment de chercher un prestataire de *cloud* pour héberger une grande quantité de données sensibles, un responsable du traitement ne pourra passer que par un sous-traitant apportant de solides garanties.

L'article 28 du RGPD précise également que « l'application, par un sous-traitant, d'un code de conduite approuvé [...] ou d'un mécanisme de certification approuvé [...] peut servir d'élément attestant de l'existence des garanties suffisantes ».

54. Si, durant la collaboration avec ce sous-traitant, le responsable du traitement remarquait que finalement son sous-traitant ne présentait plus les garanties nécessaires, il serait logiquement contraint de mettre un terme à leur relation contractuelle[98] et d'exiger du sous-traitant qu'il supprime toutes les données à caractère personnel ou les lui renvoie, et détruise les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation de ces données[99].

55. Afin de se mettre en conformité avec le RGPD, les responsables de traitement doivent s'assurer que leurs contrats de sous-traitance rédigés sous l'empire de la Directive sont toujours conformes au prescrit de l'article 28. Si tel n'est pas le cas, ils sont tenus de renégocier ceux-ci pour y intégrer les éléments manquants. Cette renégociation risque de faire augmenter le prix des prestations proposées par les sous-traitants puisque ceux-ci sont soumis à plus d'obligations qu'auparavant et assument une plus grande part de responsabilité dans les traitements auxquels ils participent.

---

[97] Pour ces différentes obligations, nous renvoyons aux autres contributions dans le présent ouvrage qui étudient spécifiquement ces points nécessitant une étude à part entière.

[98] A. Cruquenaire et J.-Fr. Henrotte, « Le devoir de conseil dans le Règlement général sur la protection des données : bis repetita placent ? », in *Law, Norms and Freedoms in cyberworld / Droit, Normes et Libertés dans le cybermonde* , *op. cit.*, p. 609.

[99] Obligation contenue à l'art. 28, § 3, g), du RGPD.

56. Notons enfin que de nombreux sous-traitants informatiques proposent leurs services sous forme de packages non négociables dont les conditions sont définies à l'avance (contrat d'adhésion). Il est donc d'autant plus important de choisir un sous-traitant qui offre un niveau de prestation suffisant.

SECTION 3. – La relation entre le responsable du traitement et son sous-traitant

§ 1. La rédaction obligatoire d'un « contrat »

57. Comme c'était déjà le cas dans la Directive[100], le responsable du traitement et le sous-traitant sont tenus de conclure un contrat[101]. Le traitement de données confié à un sous-traitant peut également être régi par « un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre » précise l'article 28, paragraphe 3, du RGPD. Cette référence au « droit d'un État membre » parait problématique parce que, comme à de nombreuses reprises dans le RGPD, il n'est jamais envisagé les possibles conflits de lois lorsque deux acteurs peuvent être soumis à des législations nationales différentes.

Cet acte juridique doit « se présenter sous une forme écrite, y compris en format électronique »[102].

Afin de rédiger cet acte juridique, les parties pourront notamment « choisir de recourir à un contrat particulier ou à des clauses contractuelles types, qui sont adoptées soit directement par la Commission soit par une autorité de contrôle »[103], ou faisant partie d'une procédure de certification délivrée au responsable du traitement[104].

58. La question reste de savoir si pareil contrat doit être conclu dans le cas où le responsable du traitement bénéficie de l'exception pour activités strictement personnelles ou domestiques. Dans ce cas précis, le sous-traitant est-il, lui, toujours obligé de conclure ce contrat avec la personne bénéficiant de l'exception et dès lors conditionner son offre de service à la conclusion de

[100] Art. 17, § 3, de la Directive.
[101] Art. 28, § 3, du RGPD.
[102] Art. 28, § 9, du RGPD.
[103] Considérant n° 81 du RGPD. Voy. art. 28, §§ 6, 7 et 8.
[104] Art. 28, § 6, du RGPD.

ce contrat ? Répondre par l'affirmative est peu réaliste puisqu'il imposerait, par exemple, à tout un chacun souhaitant utiliser un service de *cloud* public de préciser s'il va l'utiliser pour traiter des données à caractère personnel. Le RGPD ne règle pas ce cas de figure pourtant très fréquent[105].

De plus, puisque le responsable du traitement n'est pas tenu de respecter le RGPD, que devrait encore contenir ce contrat ? Si les mesures tendant à aider le responsable du traitement à respecter le RGPD semblent ne plus être adéquates vu que ce dernier n'y est pas soumis[106], qu'en est-il des autres éléments prévus à l'article 28 ?

Si l'article 28 du RGPD est inapplicable dans ce cas-là, le sous-traitant se trouvera bien souvent dans l'impossibilité de se conformer à ses propres obligations puisqu'il n'aura pas les informations nécessaires[107] afin d'apprécier le contexte dans lequel les données sont traitées. Il ne pourra donc pas, notamment, adapter son niveau de sécurité aux spécificités du traitement.

§ 2. Le contenu de ce contrat

1. Le RGPD a fortement augmenté le nombre d'éléments devant être contenus dans ce contrat. Cela force tant le responsable du traitement que son sous-traitant, dès la rédaction du contrat, à clarifier les droits et obligations de chacune des parties. De plus, via les mentions obligatoires dans les contrats de sous-traitance, le RGPD impose quelques nouvelles obligations au sous-traitant qui n'a dès lors plus la possibilité d'éviter contractuellement de devoir assumer certaines responsabilités qu'il jugerait trop contraignantes. Le sous-traitant doit donc maintenant pleinement collaborer avec son responsable du traitement, à défaut de quoi il risque lui-même dans certains cas des sanctions[108]. Face à de grands acteurs informatiques, l'article 28 offre un minimum de garanties aux responsables de traitement souhaitant faire appel à eux.

---

[105] Certains auteurs s'interrogent plus largement sur la portée du considérant 18 *in fine* du RGPD et la manière d'appliquer cette extension du champ d'application du cadre réglementaire au *cloud* public à destination des particuliers, voy. M. S. VIDOVIC, « EU data protection reform : challenges for cloud computing », http://www.cyelp.com/index.php/cyelp/article/view/252, p. 181.

[106] Nous pensons notamment à l'art. 28, § 3, e), du RGPD.

[107] Nous reviendrons sur ce point dans la section suivante.

[108] Le non respect des obligations incombant au sous-traitant (notamment celles contenues à l'article 28 du RGPD) risque d'entrainer une amende administrative « pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu », voy. art. 83, § 4, a), du RGPD.

2. Dans ce contrat, doivent notamment être précisés « l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, les obligations et les droits du responsable du traitement »[109]. Imposer la communication de cette série d'éléments permet au sous-traitant de prendre conscience du type de traitement de données dont il est question. Ainsi, celui-ci pourra facilement apprécier le caractère plus ou moins risqué du traitement et mettre en place les mesures les plus adaptées aux caractéristiques particulières de celui-ci. Le sous-traitant reste tenu par les informations qui lui ont été fournies par le responsable du traitement et n'a pas *a priori* à remettre en question la véracité de ces informations et la justesse de l'analyse quant à la nature des données traitées par exemple[110].

Rappelons que cette disposition, dans une certaine mesure, est en contradiction avec le régime d'exonération de responsabilité des hébergeurs prévue dans la directive 2000/31/CE[111]. Cette disposition priverait en effet *de facto* le sous-traitant hébergeur de l'exonération dont il bénéficie en tant que simple intermédiaire[112].

3. Le contrat doit également mentionner une série d'obligations qui incombent au sous-traitant :

- Ce dernier ne pourra « traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale [...[113]] »[114]. Très logiquement, un sous-traitant doit limiter les traitements qu'il effectue à ce qui lui est expressément demandé par son responsable du traitement. Dans les cas où les sous-traitants ne traitent pas eux-mêmes activement les données et ne font que mettre à disposition du responsable du traitement une infrastructure et des logiciels (les services de *cloud* par exemple), et ne reçoivent dès lors pas véritablement d'instructions,

---

[109] Art. 28, § 3, du RGPD.

[110] Dans le même sens voy. A. Cruquenaire et J.-F. Henrotte, « Le devoir de conseil dans le Règlement général sur la protection des données : bis repetita placent ? », *op. cit.*, p. 611.

[111] Voy. *supra*, Chapitre 6, Section 1, *in fine*.

[112] Sur ce point, voy. la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

[113] « [...] à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ».

[114] Art. 28, § 3, a), du RGPD.

cette disposition peut se comprendre comme une interdiction de traiter les données d'une manière qui serait contraire à ce que le responsable de traitement a autorisé[115].

Face à certains acteurs comme les réseaux sociaux, l'Allemagne s'est interrogée sur la « faisabilité » de cette disposition[116]. En effet, avec certains sous-traitants, les instructions pouvant être données se limitent à celles acceptées et prévues par le sous-traitant lui-même, et la possibilité de changer de sous-traitant si le refus du sous-traitant ne convient pas au responsable du traitement.

Est plus novateur dans cette disposition le fait que le RGPD ajoute maintenant l'obligation (pour le responsable du traitement) de documenter les instructions qu'il donne à son sous-traitant. Cette nouvelle condition semble donc signifier qu'un sous-traitant ne doit pas tenir compte d'instructions qu'il aurait reçues de la part de son responsable du traitement, si celles-ci ne sont pas documentées. Nous comprenons qu'un sous-traitant ait des réticences à ignorer les instructions, même non documentées, de son responsable du traitement. Néanmoins, ne pas respecter cette exigence de documentation pourrait mettre le sous-traitant dans une situation délicate vu qu'il se trouverait dans l'impossibilité de prouver qu'il a agi conformément aux instructions du responsable du traitement et qu'il ne s'est dès lors pas écarté de son rôle de sous-traitant. À défaut de pareille documentation, un sous-traitant pourrait éventuellement se voir requalifié en responsable du traitement, avec tous les inconvénients et risques que cela peut entrainer[117].

- Il devra veiller « à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité »[118]. Cet engagement sera très souvent mentionné dans le contrat de travail des employés. Pour rappel, il est également tenu de mettre en place les mesures techniques et organisationnelles permettant d'éviter toute réutilisation de ces données[119].

---

[115] W. K. Hon, E. Kosta, Chr. Millard et D. Stefanatou, « Cloud Accountability : The Likely Impact of the Proposed EU Data Protection Regulation », *op. cit.*, pp. 16 et s. et références citées.

[116] Voy. note 216 du Proposal from the Council for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), doc. 17831/13, 16 décembre 2013.

[117] Dans le même sens, voy. M. S. Vidovic, « EU data protection reform : challenges for cloud computing », *op. cit.*, p. 178.

[118] Art. 28, § 3, b), du RGPD.

[119] Art. 32, § 4, du RGPD.

- Il prendra toutes les mesures requises afin de répondre à ses obligations en matière de sécurité[120] et aidera le responsable du traitement à garantir le respect de ses propres obligations en la matière (art. 32 à 36), « compte tenu de la nature du traitement et des informations à la disposition du sous-traitant »[121]. Comme dit précédemment, le sous-traitant dispose en principe de toutes les informations nécessaires.
- Il respectera « les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant »[122]. Nous traiterons ce point spécifique dans la section suivante.
- En fonction de la nature du traitement, il aidera le responsable du traitement, « par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III »[123]. Il n'a donc pas l'obligation de répondre directement aux demandes des personnes concernées. En cas de pareille demande, il pourra éventuellement renvoyer au responsable du traitement qui est seul à même d'évaluer l'opportunité d'accéder à cette requête. Le sous-traitant n'est tenu que d'aider, techniquement, le responsable du traitement à faire droit à cette demande. Il commettrait, selon nous, une faute s'il donnait suite à une demande d'effacement, par exemple (voy. art. 17 du RGPD), qui lui serait directement adressée, sans au préalable avoir consulté le responsable du traitement. À tel point qu'il est probable que, dans ce cas, le responsable du traitement puisse se retourner contre son sous-traitant si cette initiative du sous-traitant lui était préjudiciable.
- Au terme de la prestation de services impliquant des traitements de données, il exécutera le choix du responsable du traitement de supprimer toutes les données à caractère personnel ou les renvoyer à ce dernier, et détruira les copies existantes, sauf disposition légale imposant la conservation de celles-ci[124].
- Il mettra « à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations prévues [à l'article 28 du RGPD] et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits »[125].

---

120 Art. 28, § 3, c), du RGPD. Celui-ci fait explicitement référence à l'article 32 du RGPD.
121 Art. 28, § 3, f), du RGPD.
122 Art. 28, § 3, d), du RGPD.
123 Art. 28, § 3, e), du RGPD.
124 Art. 28, § 3, g), du RGPD.
125 Art. 28, § 3, h), du RGPD.

- Il informera « immédiatement le responsable du traitement si, selon lui, une instruction de celui-ci constitue une violation du [RGPD] ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données »[126]. Précisons que cette phrase commence par « En ce qui concerne le point h) du premier alinéa ». La référence au point h) semble indiquer que « ce devoir de conseil » fait en réalité partie du devoir d'information mis à charge du sous-traitant vis-à-vis du responsable du traitement. Le sous-traitant a donc désormais l'obligation de signaler l'illégalité d'une instruction qu'il aurait constatée. Il s'agit donc d'« une obligation de conseil passive ou négative, puisqu'elle n'exige pas du sous-traitant qu'il conseille, mais plutôt qu'il déconseille »[127]. Cette nouvelle obligation impose au sous-traitant de sortir de sa position de simple exécutant à qui on ne demande pas de se poser des questions sur la légalité des traitements qu'il effectue.

  Désormais, il doit donc vérifier d'une certaine manière ce que le responsable du traitement lui demande de faire. *A priori* le sous-traitant doit disposer de suffisamment d'informations factuelles[128] pour détecter la majorité des infractions qui pourraient être commises. Concrètement, le sous-traitant a d'autant plus intérêt à signaler ces manquements qu'il risque d'engager sa responsabilité civile s'il ne le fait pas[129]. Il devra également se ménager la preuve de la réponse du responsable du traitement si celui-ci décide d'ignorer ses avertissements[130].

  Cependant, cette mesure ne doit pas avoir pour effet d'inverser les rôles. Le responsable du traitement ne peut se reposer uniquement sur ce nouveau garde-fou pour s'assurer que les instructions qu'il donne à son sous-traitant respectent le cadre règlementaire, d'autant plus que ce « devoir de conseil » ressemble plus à une obligation de moyen que de résultat.

§ 3. La question de la sous-traitance en cascade

4. Dans un monde où les traitements de données sont de plus en plus complexes, il arrive régulièrement qu'un sous-traitant fasse lui-même appel à un ou plusieurs autre(s) sous-traitant(s) pour réaliser les missions qui lui ont été confiées par le responsable du traitement.

---

126 Art. 28, § 3, al. 2, du RGPD.

127 A. Cruquenaire et J.-Fr. Henrotte, « Le devoir de conseil dans le Règlement général sur la protection des données : bis repetita placent ? », *op. cit.*, p. 612.

128 Voy. *supra*. dans cette section.

129 Voy. art. 82, § 2, du RGPD.

130 A. Cruquenaire et J.-Fr. Henrotte, « Le devoir de conseil dans le Règlement général sur la protection des données : bis repetita placent ? », *op. cit.*, p. 613. Les éventuelles conséquences pour le sous-traitant dans pareilles situations sont également étudiées dans cette contribution.

Tel est, par exemple, le cas lorsqu'une entreprise désireuse de mieux connaitre ses clients (responsable du traitement) a recours au service d'une société spécialisée dans la relation clientèle (sous-traitant initial) pour mettre en place un site web permettant à ces clients de donner leur avis. Bien souvent, cette société va elle-même faire appel à une troisième entreprise (sous-traitant secondaire) qui se chargera de l'hébergement de ce site web.

5. Afin d'éviter qu'un sous-traitant puisse lui-même sous-traiter certaines parties du traitement de données à une entreprise sans que le responsable du traitement ne soit au courant, le sous-traitant initial devra demander l'autorisation préalable, par écrit, du responsable du traitement avant de lui-même recruter un autre sous-traitant. Cette autorisation peut être spécifique (le responsable du traitement autorise le recours à un autre sous-traitant spécifique) ou générale. Dans ce second cas, le responsable du traitement doit être informé de tout changement de sous-traitant qui aurait lieu, lui laissant ainsi la possibilité « d'émettre des objections » quant à ces changements[131].

6. Avant de recruter lui-même un sous-traitant, le sous-traitant initial aura l'obligation d'imposer contractuellement[132] à ce nouvel acteur les mêmes obligations en matière de protection des données que celles incluses dans le contrat entre lui, sous-traitant initial, et le responsable du traitement[133], de sorte que le niveau de garanties offert ne s'en trouve pas affecté[134]. Le RGPD ne détaille néanmoins pas plus la relation directe entre le responsable du traitement et le sous-traitant secondaire.

7. Malgré ce nouveau contrat et l'autorisation accordée par le responsable du traitement, le sous-traitant initial « demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations »[135]. Ce nouveau sous-traitant est également tenu de respecter l'ensemble des obligations qui incombent aux sous-traitants et devra notamment, dans certains cas, tenir un registre, désigner un DPO… et pourrait être personnellement responsable civilement en cas de manquement à ses obligations[136].

---

[131] Art. 28, § 2, du RGPD. Il aurait été plus clair de parler de « possibilité de s'opposer ». Dans la version anglaise, il est d'ailleurs écrit « *opportunity to object* ».

[132] Que cela soit « par contrat ou par un autre acte juridique au titre du droit de l'Union ou d'un État membre », voy. art. 28, § 4, du RGPD.

[133] Obligations contenues à l'article 28, § 3, du RGPD.

[134] Art. 28, § 4, du RGPD.

[135] Art. 28, § 4, al. 2, du RGPD.

[136] Sur ce point, nous renvoyons à nouveau à la contribution de K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » au sein du présent ouvrage.

Conclusion

8. Le RGPD consacre désormais le principe d'« *accountability* ». Il était certes déjà sous-jacent dans la Directive, mais le règlement en fait maintenant un pilier de la règlementation relative à la protection des données.

Afin d'assurer une plus grande effectivité à cette législation, le RGPD tend donc à davantage responsabiliser le responsable du traitement. Responsabiliser celui-ci signifie concrètement qu'il a désormais plus de marge de manœuvre pour mettre en place les mesures nécessaires au respect du cadre légal. En contrepartie, le responsable du traitement doit pouvoir prouver, documents à l'appui, que les traitements qu'il effectue respectent le RGPD.

Dorénavant soumis à certaines obligations spécifiques, le sous-traitant est lui aussi responsabilisé. Il doit coopérer plus activement avec son responsable du traitement et aider ce dernier à se conformer au règlement.

9. Soucieux de ne pas laisser complètement libres les responsables de traitement et afin de leur fournir, de force, certains outils utiles, le RGPD leur impose néanmoins d'intégrer dans leur processus une série de nouveaux principes tels que le principe de « *privacy by design* » et de « *privacy by default* ».

10. À côté de ces principes encore assez vagues quand il faut les mettre en pratique, et toujours dans un souci de rendre la plus effective possible cette législation, le RGPD tente également de mieux règlementer les relations souvent complexes entre les différents acteurs d'un traitement de données, entre responsables conjoints de traitement, entre responsable du traitement et sous-traitant et même entre sous-traitant et sous-traitant du sous-traitant. Ainsi, il est imposé la conclusion d'un accord écrit entre ces différentes parties, accord dont le contenu minimum est précisé dans le règlement.

11. D'un point de vue théorique, cette obligation s'inscrit dans une certaine logique, puisque chaque acteur a des obligations et que le RGPD impose à ceux-ci de se coordonner afin d'éviter que la multiplication des acteurs ne vienne mettre en danger l'effectivité du règlement. Malheureusement, d'un point de vue pratique, la réalité est un peu différente, et ce pour différentes raisons.

Tout d'abord, dans un souci de continuité les notions de « responsable du traitement », de « sous-traitant » et de « responsables conjoints »

n'ont pas été modifiées par le RGPD et la qualification des acteurs reste parfois une opération délicate, ce qui provoque une profonde insécurité juridique. Dans la mise en œuvre, on note toutefois que la plus grande responsabilisation du sous-traitant tend à légèrement diminuer cette différence de statut puisque le sous-traitant est maintenant lui aussi directement responsable d'une série de mesures imposées par le RGPD.

12. Ensuite, dans le secteur du numérique et particulièrement des services fonctionnant sur la base de *cloud,* les sous-traitants sont devenus plus puissants économiquement et plus spécialisés que les responsables de traitant faisant appel à leurs services. Il est donc difficile de parler de véritable coordination avec ce type d'acteurs. À cela s'ajoute que, dans certains cas, ces acteurs sont des hébergeurs au sens de la directive 2001/31/CE et que les dispositions supposées coordonner cette directive et le RGPD sont peu claires.

Le problème du rapport de force se pose également entre certains responsables conjoints où un de ceux-ci, parfois incontournable sur le marché, fixe ses conditions de manière unilatérale. L'affaire de la *Fan page* sur Facebook tranchée récemment par la C.J.U.E[137]. en est le parfait exemple.

13. Enfin, le cas où le responsable du traitement bénéficie de l'exception à des fins strictement personnelles ou domestiques n'est pas suffisamment traité dans le RGPD de sorte qu'on ignore comment son sous-traitant ou son responsable conjoint sont supposés se coordonner avec cet acteur pour le moins peu concerné par le respect du RGPD.

14. Loin de nous l'idée de tirer à boulets rouges sur ce nouveau texte, avant même qu'il ait eu le temps d'être mis en pratique. Il ne règle pas tous les problèmes déjà existants sous l'empire de la Directive et certaines nouveautés manquent certes encore de précision. Mais n'est-ce pas en partie inévitable quand on considère la diversité des traitements auxquels le RGPD doit s'appliquer ? Soyons dès lors constructif. Laissons donc chaque secteur s'approprier le texte et le Comité européen de la protection des données et la Cour de justice lui donner tout son sens.

[137] C.J.U.E., arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, précité.